МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б. Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С. Т. Князев

«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ ДЕЯТЕЛЬНОСТИ БАНКОВ

Перечень сведений о рабочей программе модуля	Учетные данные
Модуль Информационная безопасность финансовой деятельности банков	**Код модуля1140584** **Учебный план №** 09.03.04/03.01
Образовательная программа Информационно аналитические системы безопасности	**Код ОП** 10.05.04/01.01
Направление подготовки Информационная безопасность финансовых и экономических структур	**Код направления и уровня подготовки** 10.05.04
Уровень образования Высшее образование – специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 01.12.2016 №1514

Екатеринбург, 2017

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	к.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля А.В. Бакланов

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий-РТФ

Председатель учебно-методического совета Н.В. Папуловская

Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль А.В. Бакланов

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ ДЕЯТЕЛЬНОСТИ БАНКОВ

1.1. Объем модуля 12 з.е.

1.2. Аннотация содержания модуля

Освоение необходимых компетенций достигается путем применения образовательных технологий, предполагающих активную самостоятельную деятельность студента – проблемного обучения, аудиторной и внеаудиторной групповой работы, – а также одновременного обращения к результатам научных исследований и анализу конкретной социальной практики (документов, событий). Специфика дисциплины состоит в формировании представления об основных принципах
организации государственной службы и кадровой политики в Российской Федерации, творческого отношения к освоению отечественного и мирового опыта организации государственной службы, умения использовать его в практической деятельности.

В модуле рассматриваются основные нормативно-методические документы в области обеспечения физической и финансовой защиты объектов финансовой сферы, способы моделирования угроз и нарушителей, строение и функционирование средств охранной сигнализации, средств контроля и управления доступом, а также средств телевизионного наблюдения.

Модуль посвящен изучению средств физической защиты объектов банка, в частности средств инженерно-технического укрепления и средств охранной сигнализации, рассматриваются основные нормативно-методические документы в области обеспечения физической защиты объектов финансовой сферы, способы моделирования угроз и нарушителей, строение и функционирование средств охранной сигнализации, средств контроля и управления доступом, а также средств телевизионного наблюдения.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС)		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля								
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Проект по модулю	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1.	**(ВС)** Безопасность дистанционного банковского обслуживания	10	34	34	-	68	76	0	Экзамен 18	144	4
2.	**(ВС)** Система физической защиты банков	10	34	34	-	68	76	0	Экзамен 18	144	4
3.	**(ВС)** Финансовые преступления в сфере информационных	10	34	34	-	68	76	0	Экзамен 18	144	4

	технологий										
Всего на освоение модуля			102	102	0	204	128	0	54	432	9

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	Безопасность дистанционного банковского обслуживания Система физической защиты банков Финансовые преступления в сфере информационных технологий
3.2.	**Кореквизиты**	

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Код результата обучения	Результаты обучения	Компетенции, формируемые в рамках достижения результатов обучения
РО-1	*Способность применять методы, средства и технологии анализа информации, обеспечивать предупреждение правонарушений и мониторинг процессов в социально-экономической, финансовой и правоохранительной сферах в рамках информационно-аналитической деятельности*	− способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3); − способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7); − способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9); − способность корректно применять аппарат математического анализа, геометрии, алгебры, дискретной математики, теории вероятностей, математической статистики, численных методов, методов оптимизации для формализации и решения задач в сфере профессиональной деятельности (ОПК-2); − способность применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности (ОПК-3); − способность применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7); − способность ориентироваться в особенностях налоговых систем и механизмах налогообложения в Российской Федерации и других странах (ОПК-9); − способность применять методы экономического анализа (ОПК-10); − способность анализировать и формализовывать поставленные задачи, выдвигать гипотезы, устанавливать границы их применения и подтверждать или опровергать их на практике (ПК-1); − способность применять методы анализа массивов данных и интерпретировать профессиональный смысл получаемых формальных результатов (ПК-2);
РО- 2	*Способность планировать, проводить исследование и разработку мероприятий по проектам в различных*	− способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1); − способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5); − способность к самоорганизации и самообразованию (ОК-8);

	отраслях экономики, осуществлять подготовку презентаций и защиту результатов исследования в рамках научно-исследовательской деятельности	− способность анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности (ОПК-1); − способность применять методы экономического анализа (ОПК-10); − способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-3); − способность применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами (ПК-4); − способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5); − способность готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований (ПК-6);
РО-3	*Способность применять методы, средства и технологии проектирования информационно-аналитических систем и разрабатывать защитные механизмы и средства обеспечения информационной безопасности в рамках проектной деятельности*	− способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5); − способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7); − способность корректно применять аппарат математического анализа, геометрии, алгебры, дискретной математики, теории вероятностей, математической статистики, численных методов, методов оптимизации для формализации и решения задач в сфере профессиональной деятельности (ОПК-2); − способность применять в профессиональной деятельности языки и системы программирования, инструментальные средства разработки программного обеспечения, современные методы и технологии программирования (ОПК-4); − способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5); − способность проводить предпроектное обследование профессиональной деятельности и информационных потребностей автоматизируемых подразделений (ПК-7); − способность разрабатывать и исследовать модели технологических процессов обработки информации в специальных ИАС (ПК-8); − способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9); − способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10); − способность разрабатывать проектные документы на создава-

		емые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11); − способность разрабатывать программное и иные виды обеспечения специальных ИАС (ПК-12); − способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-13);
РО-4	*Способность применять информационно-аналитические системы и предпринимать меры и средства обеспечения информационной безопасности в рамках в эксплуатационно-технологической деятельности*	− способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6); − способность применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности (ОПК-3); − способность применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7); − способность использовать специальные ИАС для решения задач в сфере профессиональной деятельности (ПК-14); − способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15);
РО-5	*Способность организовать, контролировать и регулировать трудовую деятельность персонала, рабочих групп, коллектива подчиненных в рамках организационно-управленческой деятельности*	− способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6); − способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6); − способность разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности (ПК-16); − способность организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-17);
РО- 6	*Способность применять, основываясь на нормативно-правовые, документы методы и средства по обеспечению информационной безопасности и защиты интересов личности,*	− способность использовать основы правовых знаний в различных сферах деятельности (ОК-4); − способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5); − способность ориентироваться в бюджетной системе страны и моделях ее построения (ОПК-8); − способность ориентироваться в особенностях налоговых систем и механизмах налогообложения в Российской Федерации и других странах (ОПК-9); − способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные (ПК-18); − способность обосновывать решения, связанные с реализацией

	общества и государства в рамках в правоохранительной деятельности.	правовых норм в пределах должностных обязанностей (ПК-19); – способность анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства (ПК-20).
РО-7	*Способность анализировать и обеспечивать информационную безопасность финансовых и экономических структур (для специализации №2 «Информационная безопасность финансовых и экономических структур»)*	– способность использовать основы экономических знаний в различных сферах деятельности (ОК-2); – способность применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7); – способность применять методы экономического анализа (ОПК-10); – способность проводить комплексный анализ функционирования финансовых и экономических структур государственного или системообразующего уровня с целью выявления угроз (отрицательных тенденций) национальной безопасности Российской Федерации (ПСК-2.1); – способность выполнять анализ корректности и устойчивости функционирования отдельных компонентов, подсистем и в целом всей национальной системы по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма (ПСК-2.2); – способность решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности (ПСК-2.3); – способность разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени (ПСК-2.4);

4.2. Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ПК-9	ПСК-2.4	ОПК-3	ПК-2
1	**(ВС)** Безопасность дистанционного банковского обслуживания	*	*		
2	**(ВС)** Система физической защиты банков			*	
3	**(ВС)** Финансовые преступления в сфере информационных технологий	*			*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:
Не предусмотрено

5.2. Форма промежуточной аттестации по модулю:
Не предусмотрено

5.3. Фонд оценочных средств для проведения промежуточной аттестации по модулю (Приложение 1)

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю

Не предусмотрено

5.3.2.2. Перечень примерных тем итоговых проектов по модулю

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России
Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Информационная безопасность финансовой деятельности банков	**Код модуля1140584** **Учебный план №** 6938
Образовательная программа Информационно аналитические системы безопасности	**Код ОП** 10.05.04/01.01
Направление подготовки Информационная безопасность финансовых и экономических структур	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки Высшее образование – специалитет	
ФГОС ВО 10.05.04 Информационно аналитические системы безопасности	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 01.12.2016 №1514

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	К.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам. председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

1.1.Аннотация содержания дисциплины

Задачи дисциплины «Финансовые преступления в сфере информационных технологий» - дать знания по вопросам:

- обеспечения информационной безопасности государства;
- процессов сбора, передачи и накопления информации;
- методов и средств ведения информационных войн.

В дисциплине рассматриваются основные нормативно-методические документы в области обеспечения физической защиты объектов финансовой сферы, способы моделирования угроз и нарушителей, строение и функционирование средств охранной сигнализации, средств контроля и управления доступом, а также средств телевизионного наблюдения.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-3);
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);
- способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные (ПК-18);
- способность обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей (ПК-19);
- способность анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства (ПК-20).
- способность проводить комплексный анализ функционирования финансовых и экономических структур государственного или системообразующего уровня с целью выявления угроз (отрицательных тенденций) национальной безопасности Российской Федерации (ПСК-2.1);
- способность решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности (ПСК-2.3);
- способность разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени (ПСК-2.4).

В результате освоения дисциплины студент должен:

Знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности государства;
- основные термины по проблематике информационной безопасности;

- методологию создания систем защиты информации;
- перспективные направления развития средств и методов защиты информации;
- роль и место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства;
- содержание информационной войны, методы и средства ее ведения;

Уметь:

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;

Владеть (демонстрировать навыки и опыт деятельности):

- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего Часов	В т.ч. контактная работа (час.)*	*10*
1.	**Аудиторные занятия**	**68**	**68**	**68**
2.	Лекции	34	34	34
3.	Практические занятия	34	34	34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**58**	**10,20**	**58**
6.	**Промежуточная аттестация**	**18**	**0,25**	**18**
7.	**Общий объем по учебному плану, час.**	**144**	**78,45**	**144**
8.	**Общий объем по учебному плану, з.е.**	**4**		**4**

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.
2	Информационная война, методы и средства ее ведения	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.
3	**Платежные терминалы**	Классификация платежных терминалов по функциональным возможностям. Агентская и банковская схемы функционирования. Функциональные части и их назначение. Корпус платежного терминала, модем для организации обмена информацией между платежным терминалом и сервером электронной платежной системы. Конструктивные особенности Безопасность платежных терминалов. Этапы работы платежных терминалов.
4	**Основные виды угроз в отношении Банкоматов и платежных терминалов.**	Общие критерии формирования модели нарушителя. Типология нарушителей. Категории нарушителей и виды совершаемых преступлений. Цели нарушителей. Оценка опасности нарушителя исходя из степени его осведомленности, оснащенности и подготовленности, типология нарушителей по подготовленности к преодолению системы охраны. Категории нарушителей и виды совершаемых ими преступлений, связанных с незаконным проникновением в зону размещения банкоматов и

		платежных терминалов, криминальными посягательствами и конфиденциальную информацию банкоматов, а также на пользователей платежных терминалов и банкоматов, инкассаторов и обслуживающий персонал. Квалификация преступления. Угрозы держателю карты, обслуживающему персоналу. Нападение. Неправомерный доступ к Персональным данным. Угрозы банковской карте, ее реквизитам. Скимминг. Шимминг. Траппинг. Угрозы банкоматам и платежным терминалам. Несанкционированное проникновение на территорию, в здание, где установлены платежные терминалы и банкоматы. Вскрытие банкоматов. Хищение, срыв с места установки.
5	**Обеспечение безопасности платежных терминалов и банкоматов**	Требования Положения ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов. Основные организационные и технические меры по защите информации банкоматов и платежных терминалов. Выбор мест размещения банковских устройств самообслуживания. Влияние категории на место размещения. Анализ уязвимостей программного обеспечения банкоматов и терминалов. Обеспечение фиксации. Инженерно-техническая укрепленность и оборудование техническими средствами охраны банковских устройств самообслуживания и мест их размещения. Регулирование и установка порядков срока хранения информации, обновления версий, работы с клиентами. Оценка времени взлома. Минимальные требования по устойчивости к взлому сейфов. Системы удаленного мониторинга состояния устройства, обеспечивающие контроль надлежащего функционирования защитного оборудования и специального программного обеспечения. Требования к системе передачи тревожных сообщений для защиты банкоматов и платежных терминалов. Фиксация фактов атак и попыток их совершения. Информирование Банка России. Информирование населения.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 12
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Информационная безопасность в системе национальной безопасности Российской Федерации	7	5	5			2	2	2																				
2	Информационная война, методы и средства ее ведения	20	12	8	4		8	5	3		2														3	1				
3	Платежные терминалы	22	13	8	5		9	6	4		2														3	1				
4	Основные виды угроз в отношении банкоматов и платежных терминалов	28	20	9	11		8	8	3		5																			
5	Обеспечение безопасности платежных терминалов и банкоматов	32	18	4	14		14	8	4		4		6	1																
	Всего (час), без учета промежуточной аттестации:	109	68	34	34		41	29	16		13		6	6											6	6				
	Всего по дисциплине (час.):	**144**	**68**				**58**	В т.ч. промежуточная аттестация																				**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Номер работы	Раздел, тема дисциплины	Наименование работы	Объем учебного времени, час.
1	Т2	Информационная война, методы и средства ее ведения	4
2	.Т 3	Платежные терминалы	5
3	Т 4	Основные виды угроз в отношении банкоматов и платежных терминалов	11
4	Т5	Обеспечение безопасности платежных терминалов и банкоматов	14
Всего			**34**

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Домашняя работа №1. *Виды защищаемой информации.*
Домашняя работа №2. *Угрозы развитию отечественной индустрии информации.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Компьютерная система как объект информационного воздействия.

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Контрольная работа №1. *Виды безопасности и сферы жизнедеятельности личности, общества и государства.*
Контрольная работа №2. *Роль информационной безопасности в обеспечении национальной безопасности государства.*
Контрольная работа №3. *Информационная безопасность и информационное противоборство.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Информационная безопасность в системе национальной безопасности Российской Федерации				*								
2. Информационная война, методы и средства ее ведения				*								
3.Платежные терминалы					*			*				
4.Основные виды угроз в отношении Банкоматов и платежных терминалов				*	*						*	
5.Обеспечение безопасности платежных терминалов и банкоматов					*						*	

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Мошенничество в платежной сфере: бизнес-энциклопедия / Центр исследований

платежных систем и расчетов ; ред.-сост. А. Воронин. - Москва : Интеллектуальная Литература, 2016. - 345 с. : табл., схем. - ISBN 978-5-99072-232-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=430951
2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605
3. Аверченков, В.И. Аудит **информационн**ой **безопасност**и : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245
4. Аудит **информационн**ой **безопасност**и органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 4-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 100 с. - (Организация и технология защиты информации). - Библиогр.: с. 83-84. - ISBN 978-5-9765-1277-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259
5. Башлы, П.Н. **Информационная безопасность** : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - Москва : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539

9.1.2. Дополнительная литература

1. Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие для вузов / В. А. Галатенко ; Под ред. В. Б. Бетелина .— 3-е изд., испр. — М. : Интернет-Ун-т Информ. Технологий, 2006 .— 208 с. — (Основы информационных технологий). — Рек. Учеб.-метод. об-нием в обл. прикладной информатики .— Библиогр.: с. 256-260. — ISBN 5-9556-0015-9 : 200-00. + URL: http://biblioclub.ru/index.php?page=book&id=233063
2. Спицын, В.Г. **Информационная безопасность** вычислительной техники : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил.,табл., схем. - ISBN 978-5-4332-0020-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208694
3. Сычев, Ю.Н. Основы **информационн**ой **безопасност**и : учебно-практическое пособие / Ю.Н. Сычев. - Москва : Евразийский открытый институт, 2010. - 328 с. - ISBN 978-5-374-00381-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90790

9.2. Методические разработки

1. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В. — 2007. — Курс "Основы информационной безопасности" является по своей сути введением в специальность "Компьютерная безопасность". Рассматриваются исторически сложившиеся направления информационной защиты. Излагаются качественные модели информационной защиты. Обсуждаются информационные преступления и информационные войны. Включает учебное пособие, программу дисциплины,

экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11063>.

2. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В., Вострецова Е.В., Гайдамакин Н.А., Лучинин А.С. — УМК. — 2010 .— Дисциплина «Основы информационной безопасности» имеет целью обучить студентов принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем. «Основы информационной безопасности» в соответствии с государственными образовательными стандартами является обязательной дисциплиной для специальности Информационная безопасность телекоммуникационных систем. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=9407>.

9.3. Программное обеспечение

MS Office

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.urfu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.urfu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.urfu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.urfu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.urfu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*10,1-7*	*20*
Домашняя работа №2	*10,8-15*	*20*
Контрольная работа №1	*10,1-7*	*30*
Контрольная работа №2	*10,8-15*	*30*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям–** *не предусмотрена*		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0,5		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 10	**1**

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с наличием Дисциплины и ее аналогов, по которым возможно тестирование, на портале СМУДС УрФУ, возможно тестирование в рамках НТК.

ПРИЛОЖЕНИЕ 3

к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	Пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи для домашних заданий

Домашняя работа №1.

1) *Укажите классификацию видов защищаемой информации.*

2) *Приведите описание интересов государства в информационной сфере в соответствии с нормативными документами.*

Домашняя работа №2.

1) *Укажите угрозы индустрии средств информатизации, телекоммуникации и связи,*

2) *Укажите угрозы обеспечению потребностей внутреннего рынка в информационной продукции и выходу этой продукции на мировой рынок,*

3) *Укажите угрозы обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.*

Примерные контрольные задачи в рамках контрольных работ

Контрольная работа №1.

1) *Опишите виды экономической и внутриполитической безопасности общества и государства,*

2) *Опишите виды социальной и международной безопасности общества и государства,*

3) *Опишите виды информационной, военной и пограничной безопасности общества и государства.*

Контрольная работа №2.

1) *Приведите классификацию угроз компьютерной информации.*

2) *Приведите классификацию ущерба компьютерной информации.*

3) *Опишите роль информационной безопасности в обеспечении национальной безопасности государства.*

Контрольная работа №3. *Информационная безопасность и информационное противоборство.*

1) *Опишите субъекты и цели информационного противоборства.*

2) *Дайте классификацию методов информационного противоборства.*

3) *Дайте классификацию видов и возможностей информационного оружия.*

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы общества в информационной сфере.
8. Интересы государства в информационной сфере.
9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
10. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
11. Угрозы информационному обеспечению государственной политики Российской Федерации.
12. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
13. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
14. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства.
15. Содержание информационного противоборства на межгосударственном уровне
16. Информационная безопасность и информационное противоборство.
17. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства.
18. Информационное оружие, его классификация и возможности.
19. Компьютерная система как объект информационного воздействия.
20. Компьютерная система как объект информационной безопасности.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России
Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ БАНКОВ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Информационная безопасность финансовой деятельности банков	**Код модуля1140584** **Учебный план №** 6938
Образовательная программа Информационно аналитические системы безопасности	**Код ОП** 10.05.04/01.01
Направление подготовки Информационная безопасность финансовых и экономических структур	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки Высшее образование – специалитет	
ФГОС ВО 10.05.04 Информационно аналитические системы безопасности	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 01.12.2016 №1514

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	К.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам. председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ БАНКОВ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению средств физической защиты объектов банка, в частности средств инженерно-технического укрепления и средств охранной сигнализации. В дисциплине рассматриваются основные нормативно-методические документы в области обеспечения физической защиты объектов финансовой сферы, способы моделирования угроз и нарушителей, строение и функционирование средств охранной сигнализации, средств контроля и управления доступом, а также средств телевизионного наблюдения. Изучаются наиболее распространенные промышленные образцы технических средств отечественного и иностранного производства, а также излагаются организационные вопросы обеспечения безопасности денежных средств работниками объектов финансовой сферы.

1.2. Язык реализации программы – русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-3);
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);
- способность обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей (ПК-19);
- способность анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства (ПК-20).
- способность выполнять анализ корректности и устойчивости функционирования отдельных компонентов, подсистем и в целом всей национальной системы по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма (ПСК-2.2);

В результате освоения дисциплины студент должен:

Знать:

- нормативные документы Министерства Внутренних Дел Российской Федерации и Банка России об инженерно-технической защите зданий, сооружений, кассовых узлов и хранилищ ценностей;
- Государственные стандарты в области обеспечения физической защиты объектов финансовой сферы;
- характеристики механической прочности строительных материалов, применяемых при возведении объектов финансовой сферы, а также их структурных компонентов;
- основы функционирования и устройства замков и иных запорных устройств;
- методы испытаний защитных конструкций в соответствии с Государственными

стандартами Российской Федерации;
- требования по инженерно-технической укрепленности зданий и помещений объектов финансовой сферы (банков, а также их функциональных служб и подразделений);
- требования по инженерно-технической укрепленности пунктов обмена денежных средств, платежных терминалов и банкоматов;
- основные характеристики и принципы построения средств охранной и пожарной сигнализации объектов финансовой сферы;
- требования, предъявляемые к средствам телевизионного наблюдения;
- основные характеристики, особенности, а также преимущества и недостатки биометрических систем идентификации и аутентификации сотрудников и должностных лиц объектов финансовой сферы.
- тактику действий нарушителей безопасности;
- основные категории и цели нарушителей физической безопасности;
- основные способы криминального взлома ограждающих и защитных сооружений объектов финансовой сферы;
- наиболее распространенные инструменты и технические средства, применяемые нарушителями физической защищенности объектов финансовой сферы;

Уметь:
- выполнять предпроектные изыскания по оборудованию зданий и помещений объектов финансовой сферы;
- проводить испытания элементов инженерно-технического укрепления объектов финансовой сферы;
- организовывать и координировать работы по инженерно-техническому укреплению зданий и сооружений объектов финансовой сферы.
- оценивать стоимость средств инженерно-технической укрепленности объектов финансовой сферы;
- осуществлять подбор и приобретение оборудования для оснащения зданий и помещений объектов финансовой сферы (банков, пунктов обмена валюты, банкоматов и платежных терминалов);
- осуществлять подбор строительных материалов и конструкций для усиления стен, перекрытий, остекленных поверхностей и дверей для объектов финансовой сферы;
- оценивать прочность и эффективность сдерживания нарушителей основных строительных конструкций и ограждающих поверхностей;
- оценивать состояние строительных конструкций и ограждающих поверхностей;
- рассчитывать вероятное время преодоления строительных конструкций и инженерно-технических сооружений нарушителем;
- анализировать возможные исходы доступа нарушителей к объектам финансовой сферы в различных ситуациях;

Владеть (демонстрировать навыки и опыт деятельности):
- профессиональной терминологией в области обеспечения физической безопасности объектов финансовой сферы;
- методами обеспечения безопасности объектов финансовой сферы;
- методами оценки значений времени преодоления инженерно-технических укреплений и рубежей защиты;
- методами оценки эффективности отечественных и зарубежных средств обеспечения физической защиты;
- методами проектирования комплексной системы физической защиты объектов финансовой сферы;
- способами описания тактики и целей нарушителя;
- навыками моделирования угроз физической безопасности;
- навыками составления организационно-распорядительных документов в области

осуществления физической защиты объектов финансовой сферы для сотрудников и должностных лиц.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего Часов	В т.ч. контактная работа (час.)*	*10*
1.	**Аудиторные занятия**	**68**	**68**	**68**
2.	Лекции	34	34	34
3.	Практические занятия	34	34	34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**58**	**10,20**	**58**
6.	**Промежуточная аттестация**	**18**	**0,25**	**18**
7.	**Общий объем по учебному плану, час.**	**144**	**78,45**	**144**
8.	**Общий объем по учебному плану, з.е.**	**4**		**4**

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	**Основные термины и определения в области защиты информации**	Основные термины и определения в области защиты информации (защита информации, техническая защита информации, физическая защита информации, организационные мероприятия по обеспечению физической защиты информации, система защиты информации, объект защиты информации, средство физической защиты информации, оценка соответствия требованиям по защите информации).
Р2	**Проектирование средств инженерно-технической укрепленности объектов финансовой сферы**	Проектирование систем сопротивления физическому вторжению на объекты финансовой сферы. Нормативные документы по оборудованию зданий, помещений, кассовых узлов и хранилищ. Периметровые ограждения. Строительные нормы и правила оборудования зданий и помещений, предназначенных для хранения денег. Требования к ограждающим конструкциям зданий и помещений. Оборудование оконных проемов, к которым возможен наружный доступ. Требования к защитным решеткам. Виды специальных стекол. Требования к оборудованию дверных проемов. Замковые устройства и ключи повышенной секретности. Оборудование вентиляционных каналов. Проектирование рубежей сдерживания нарушителя. Оценка времени сдерживания и трудоемкости строительства и эксплуатации рубежей. Требования к сдерживающим и эстетическим характеристикам механических препятствий.
Р3	**Моделирование угроз и нарушителей**	Классификация информационных нарушителей. Категории информационных нарушителей. Цели нарушителей. Оценка опасности нарушителя исходя из степени его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя. Общая характеристика удаленного доступа на объект информатизации. Реализация атак с маловероятным исходом. Возможность атак с использованием промежуточных узлов и территорий. Оценка риска удаленного доступа для объекта атаки и нарушителя. Непосредственные атаки на объекты информатизации. Виды непосредственных атак, связанных с внедрением нарушителя, использованием аппаратных и программных закладок. Преимущества и недостатки непосредственного доступа. Геометрическая модель нарушителя. Характерные

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		антропометрические размеры человеческого тела в статических положениях и в движении. Учет геометрической модели нарушителя при проектировании систем видеонаблюдения, чувствительных зон и заграждений сигнализационных датчиков. Биомеханическая модель человека. Силовые и скоростные реакции. Способы перемещения человека в пространстве. Локомоции и их виды. Учет силовых и скоростных характеристик человека при проектировании механических препятствий и рубежей сдерживания. Физико-химическая модель человеческого тела. Проводимость человеческого тела. Электризация биологических тканей в электростатическом поле. Диэлектрическая проницаемость человеческого тела. Статическая электризация тела и одежды при движении. Характеристика инфракрасного излучения теплокровных организмов. Воздействие человеческого тела на внешние поля электромагнитной и акустической энергии. Социальная модель. Использование нарушителем инструментов для взлома. Приспособления, используемые преступниками для разрушения периметров, стен зданий и помещений, дверей, оконных решеток и др. Демаскирующие признаки веществ, материалов, инструмента и принадлежностей, используемых информационными нарушителями. Демаскирующие признаки нарушителя, позволяющие его обнаружить и идентифицировать. Признаки присутствия и функционирования автономных средств технической разведки и вредоносных компьютерных программ. Тактика непосредственного доступа к автоматизированным системам и машинным носителям информации. Анализ возможных исходов доступа в различных ситуациях. Характерные признаки непосредственного доступа. Вероятная тактика нарушителей, определяемая целью проникновения и качеством охраны объекта. Модель поведения человека-нарушителя в экстремальных ситуациях.
Р4	**Средства охранной сигнализации**	Сигнализационные датчики охраны режимных помещений и протяженных участков (периметров объектов). Классификация, основные характеристики и конфигурация контролируемых зон сигнализационных датчиков. Принципы построения сигнализационных датчиков. Алгоритмы обработки измерительной информации в трактах сигнализационных датчиков.

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		Структура сигнализационных датчиков, приборов, систем и комплексов. Принципы построения централизованных и автономных сигнализационных систем. Преобразователи физических величин. Характеристики сигнализационных преобразователей: входные и выходные величины, функция преобразования, чувствительность. Генераторные и параметрические преобразователи. Типы преобразователей. Классификация средств обнаружения по типу преобразования физических величин. Конструктивные особенности чувствительных элементов. Сигнализационные датчики первого рубежа охраны: электроконтактные, магнитоконтактные, удароконтактные (датчики разрушения стекла). Основные характеристики и особенности применения активных и пассивных инфракрасных сигнализационных датчиков. Классификация радиотехнических средств обнаружения. Однопозиционные СВЧ-датчики для охраны помещений. Радиотехнические датчики охраны периметра объекта. Блокировка помещений и участков периметров сигнализационными датчиками емкостного типа. Ультразвуковые объемные датчики охраны помещений. Акустические датчики охраны остекленных поверхностей. Контроль поверхностей стен, перекрытий и отдельных предметов с помощью вибрационных сигнализационных датчиков. Периметровые вибрационные и сейсмические датчики. Быстроразвертываемые сигнализационные системы. Датчики охраны периметров с малозаметной линейной частью. Правила размещения на контролируемом объекте сигнализационных датчиков охраны периметров и помещений. Типовые схемы размещения чувствительных элементов сигнализационных датчиков в охраняемых помещениях. Рекомендуемые сочетания. Влияние дестабилизирующих факторов на работоспособность сигнализационных датчиков. Промышленные образцы сигнализационных изделий отечественного и зарубежного производства.
Р5	**Средства пожарной сигнализации**	Устройства и системы пожарной сигнализации. Классификация и принципы построения пожарных датчиков. Пожарные приемно-контрольные приборы (ПКП) и сигнально-пусковые устройства (СПУ). Порядок выбора и установки пожарных датчиков и ПКП на объектах, требования нормативных документов. Приемно-контрольные приборы охранно-

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		пожарной сигнализации. Классификация и основные характеристики ПКП. Обобщенная структурная схема ПКП. ПКП многопроводной (лучевой) структуры, принципы контроля состояния двухпроводных шлейфов охранной и пожарной сигнализации, основные типы регистрирующих ячеек. Адресные проводные и радиоканальные ПКП: протокол обмена данными между ПКП и периферийными устройствами, способы разделения каналов системы синхронизации. Использование радио- и электросети в качестве адресной линии связи. Промышленные образцы приемно-контрольных приборов отечественного и зарубежного производства. Системы передачи информации охранно-пожарной сигнализации. Варианты построения систем передачи тревожной информации от периферийных устройств объектовой сигнализации. Принципы построения систем передачи информации (СПИ), использующих специально выделенные и занятые (ВЧ уплотнение) линии телефонной сети общего пользования. Создание локальной радиосети для системы сигнализации. Радиоканальные системы передачи информации (РСПИ): приемо-передающая аппаратура, антенны, выбор частотного диапазона, особенности распространения радиоволн в городских условиях, радиопомехи. Использование радиолиний сотовых сетей связи общего пользования, специальных радиосетей передачи данных.
Р6	**Средства телевизионного наблюдения**	Тактические требования, предъявляемые к системам охранного телевидения. Классификация и обобщенная структура телевизионных средств наблюдения. Телевизионная аппаратура передачи и приема: видеокамеры, оптические системы (объективы), видеоконтрольные устройства (мониторы). Устройства обработки видеоизображения: коммутаторы, квадраторы, мультиплексоры, матричные коммутаторы. Анализаторы видеоизображения, видеодетекторы движения. Компьютерные средства отображения, документирования и архивирования информации. Устройства дистанционного управления видеосистемами. Управление системой телевизионного наблюдения с компьютерного терминала. Аппаратура видеодокументирования: специальные видеомагнитофоны, видеопринтеры. Вспомогательное оборудование видеосистем. Основные аспекты проектирования телевизионных систем наблюдения и охраны.

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		Особенности выбора технических средств телевизионной системы. Анализ типовых проектных решений.
Р7	**Средства контроля и управления доступом**	Основные понятия и определения. Классификация СКУД. Специальные режимы пропуска. Биометрические системы аутентификации. Биометрическая аутентификация по статическим признакам. Принципы распознавания человека по дактилоскопическому узору пальцев и форме руки. Распознавание по радужной оболочке и сетчатке глаза. Распознавание по форме головы и лица. Использование тепловой карты лица. Сведения о распознающих приборах, их характеристика. Ошибки первого и второго рода. Хранение аутентифицирующей биометрической информации в базах данных СКУД. Биометрическая аутентификация по динамическим признакам. Динамические признаки рукописного почерка. Принципы распознавания говорящего по голосу. Распознавание пользователя ЭВМ по клавиатурному почерку. Достоинства и недостатки биометрических систем. Перспективные способы аутентификации. Физические носители ключевой информации. Ключевые дискеты и оптические диски. Магнитные карты. Карты Wiegand. Proximity-карты. Устройства хранения и обработки идентифицирующей информации на основе смарт-карт. Исполнительные устройства управления доступом. Механические, электромеханические замки, автоматические шлагбаумы, турникеты, шлюзы.
Р8	**Безопасность инкассации**	Тактика преступников при ограблении инкассаторов и транспортных средств. Контрнаблюдение. Полномочия инкассаторов и работников охраны на маршрутах инкассации. Противодействие закладке взрывных устройств. Выбор маршрутов. Типовые случаи реагирования на внештатные ситуации. Действия инкассаторов в экстремальных условиях. ГОСТ Р 50963-96 «Защита броневая специальных автомобилей». Сравнительные характеристики отечественных и зарубежных транспортных средств инкассации.
Р9	**Обеспечение личной безопасности должностных лиц и сотрудников банков**	Цели злоумышленников при воздействии на должностных лиц и сотрудников объектов финансовой сферы. Основные виды угроз безопасности должностных лиц и сотрудников объектов финансовой сферы и

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		способы их осуществления. Самоохрана должностных лиц и сотрудников объектов финансовой сферы.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 12
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ.,семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Основные термины и определения в области защиты информации	5	4	4			1	1	1																				
2	Проектирование средств инженерно-технической укрепленности объектов финансовой сферы	13	8	4	4		5	3	3	2															2	1					
3	Моделирование угроз и нарушителей	18	8	2	6		10	8	4	2															2	1					
4	Средства охранной сигнализации	17	7	3	4		10	4	2	2			6	1																	
5	Средства пожарной сигнализации	11	9	3	6		2	2	1	1																					
6	Средства телевизионного наблюдения	14	11	5	6		3	3	2	1																					
7	Средства контроля и управления доступом	13	8	4	4		5	5	3	2																					
8	Безопасность инкассации	14	9	5	4		5	3	2	1															2	1					
9	Обеспечение личной безопасности должностных лиц и сотрудников банков	4	4	4																											
	Всего (час), без учета промежуточной аттестации:	109	68	34	34		41	29	18	11			6	6											6	6					
	Всего по дисциплине (час.):	**144**	**68**				**58**	В т.ч. промежуточная аттестация																				**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Описание комплекса средств инженерно-технической укрепленности объектов финансовой сферы	4
3	2	Разработка модели угроз физической безопасности объекта финансовой сферы	5
4	3	Комплексный анализ средств охранной сигнализации	5
5	4	Анализ наиболее широко используемых средств пожарной сигнализации: преимущества и недостатки	5
6	5	Анализ наиболее широко используемых средств телевизионного наблюдения: преимущества и недостатки	5
7	6	Анализ наиболее широко используемых средств контроля и управления доступом: преимущества и недостатки	5
8	7	Разработка положений инструкции инкассаторов и работников охраны на маршрутах инкассации	5
		Всего:	**34**

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

– *Сравнительный анализ средств охранной сигнализации отечественного и зарубежного производства.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

- *Основные требования, предъявляемые к объектам финансовой сферы при проектировании средств физической укрепленности;*
- *Составление актуальной модели нарушителя физической безопасности объекта финансовой сферы;*
- *Основные правила безопасной инкассации денежных средств и материальных ценностей.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1. Основные термины и определения в области защиты информации			*	*	*							
2. Проектирование средств инженерно-технической укрепленности объектов финансовой сферы				*				*				
3. Моделирование угроз и нарушителей					*			*				
4. Средства охранной сигнализации				*	*						*	
5. Средства пожарной сигнализации					*						*	
6. Средства телевизионного наблюдения			*	*	*							
7. Средства контроля и управления доступом				*				*				
8. Безопасность инкассации					*			*				
9. Обеспечение личной безопасности должностных лиц и сотрудников банков				*	*						*	

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Ясенев, В.Н. Информационные **систем**ы и технологии в экономике : учебное пособие / В.Н. Ясенев. - 3-е изд., перераб. и доп. - Москва : Юнити-Дана, 2015. - 560 с. : табл., граф., ил., схемы - Библиогр.: с. 490-497. - ISBN 978-5-238-01410-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115182
2. Чибисов, О.В. Организация и управление безопасностью в кредитно-финансовых учреждениях : учебное пособие / О.В. Чибисов. - Москва : Евразийский открытый институт, 2011. - 116 с. - ISBN 978-5-374-00544-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90667
3. Чибисов, О.В. Организация и управление безопасностью в кредитно-финансовых учреждениях : учебное пособие / О.В. Чибисов. - Москва : Евразийский открытый институт, 2011. - 116 с. - ISBN 978-5-374-00544-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90667

9.1.2.Дополнительная литература

1. Сычев, Ю.Н. Управление безопасностью и безопасность бизнеса : учебное пособие / Ю.Н. Сычев. - Москва : Московский государственный университет экономики, статистики и информатики, 2005. - 96 с. - ISBN 5-7764-0545-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90779
2. Информационная безопасность и **защита** информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - Москва : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774
3. Рождественская, Т.Э. Публичное **банков**ское право : учебник для магистров / Т.Э. Рождественская, А.Г. Гузнов ; Министерство образования и науки Российской Федерации, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). - Москва : Проспект, 2016. - 448 с. - Библиогр. в кн. - ISBN 978-5-392-21120-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=444797
4. Рождественская, Т.Э. Финансово-правовое регулирование **банков**ской деятельности : монография / Т.Э. Рождественская, А.Г. Гузнов ; Министерство образования и науки Российской Федерации, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). - Москва : Проспект, 2016. - 336 с. - Библиогр. в кн. - ISBN 978-5-392-21140- ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=444796

9.2.Методические разработки

Не предусмотрено

9.3.Программное обеспечение

MS Office

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.

3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Лекционная аудитория Р-339: Экран электрический Draper Targa; Крепление проектора потолочное Chief, длинная труба; Громкоговоритель пассивный PHD; Камера видеонаблюдения Panasonic WV-SF336E; Шкаф телекоммуникационный Euromet EU/R-12; Планшет Sharp ll-s201a;Системный блок Lenovo M73e Tiny; Коммутатор VGA Kramer VP-61xl; Архитектурный интерфейс Extron Cable Cubby 200 (проходные модули); Проектор потолочный Panasonic PT-DW740; Микрофон Shure MX412D/S12; Усилитель громкости со встроенным микшером Digisynthetic DS 450; Подавитель обратной связи Digisynthetic DS 212; Радиомикрофонная система DB 910R; Микшер Restmoment RX412;Учебная мебель на 150 рабочих мест, рабочее место преподавателя (стол, стул) доска меловая.

Аудитории для проведения лабораторных занятий: Р-440 - учебная мебель на 20 рабочих мест, стол, стул ,компьютер преподавательский-1,компьютеры pilips-12, стационарный м/медийный проектор Epson-1, доска маркерная-2; Р-445 - Учебная мебель на 13 рабочих мест-стол, стул для преподавателя,компьютеры-13 марки pilips,м/медийный проектор-1,маркерная доска-2.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,7		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа №1	*10,1-7*	*20*
Контрольная работа №2	*10,1-7*	*20*
Контрольная работа №3	*10,1-7*	*20*
Домашняя работа	*10,8-15*	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.3		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическая работа №1	*10,1-7*	*20*
Практическая работа №2	*10,1-7*	*20*
Практическая работа №3	*10,1-7*	*12*
Практическая работа №4	*10,8-15*	*12*
Практическая работа №5	*10,8-15*	*12*
Практическая работа №6	*10,8-15*	*12*
Практическая работа №7	*10,8-15*	*12*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	Коэффициент значимости результатов освоения дисциплины в семестре
Семестр 10	**1**

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с наличием Дисциплины и ее аналогов, по которым возможно тестирование, на портале СМУДС УрФУ, возможно тестирование в рамках НТК.

ПРИЛОЖЕНИЕ 3

к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	Пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Нормативные документы по инженерно-технической защите зданий, сооружений, помещений банков и их функциональных служб.
2. Требования к ограждающим конструкциям зданий и помещений, оценка состояния и методы испытаний. Основные способы криминального взлома ограждающих и защитных сооружений.
3. Требования к строительным материалам и конструкциям для усиления стен, перекрытий, остекленных поверхностей и дверей.
4. Требования к оборудованию дверных проемов. Оборудование оконных проемов, к которым возможен наружный доступ. Требования к защитным решеткам. Виды специальных стекол.
5. Устройство замков и иных запорных устройств. Ключи повышенной секретности.
6. Основы проектирования рубежей сдерживания нарушителя. Оценка времени сдерживания и трудоемкости строительства и эксплуатации рубежей. Требования к сдерживающим и эстетическим характеристикам механических препятствий.
7. Классификация информационных нарушителей (категории, цели, ресурсы).
8. Общая характеристика удаленного доступа на объект информатизации. Реализация атак с маловероятным исходом. Возможность атак с использованием промежуточных узлов и территорий.
9. Оценка опасности нарушителя исходя из степени его осведомленности, оснащенности и подготовленности. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Оценка риска удаленного доступа для объекта атаки и нарушителя.
10. Непосредственные атаки на объекты информатизации. Виды непосредственных атак, связанных с внедрением нарушителя, использованием аппаратных и программных закладок. Преимущества и недостатки непосредственного доступа.
11. Геометрическая модель нарушителя. Характерные антропометрические размеры

человеческого тела в статических положениях и в движении. Учет геометрической модели нарушителя при проектировании систем видеонаблюдения, чувствительных зон и заграждений сигнализационных датчиков.

12. Биомеханическая модель человека. Силовые и скоростные реакции. Способы перемещения человека в пространстве. Локомоции и их виды. Учет силовых и скоростных характеристик человека при проектировании механических препятствий и рубежей сдерживания.
13. Физико-химическая модель человеческого тела. Проводимость, диэлектрическая проницаемость, инфракрасное излучение теплокровных организмов. Воздействие человеческого тела на внешние поля электромагнитной и акустической энергии.
14. Социальная модель. Использование нарушителем инструментов для взлома, разрушения периметров, стен зданий и помещений, дверей, оконных решеток и др.
15. Демаскирующие признаки материалов и инструментов, используемых информационными нарушителями. Демаскирующие признаки нарушителя, позволяющие его обнаружить и идентифицировать. Признаки присутствия и функционирования автономных средств технической разведки и вредоносных компьютерных программ.
16. Тактика непосредственного доступа к автоматизированным системам и машинным носителям информации. Анализ возможных исходов доступа в различных ситуациях. Характерные признаки непосредственного доступа.
17. Вероятная тактика нарушителей, определяемая целью проникновения и качеством охраны объекта. Модель поведения человека-нарушителя в экстремальных ситуациях.
18. Преобразователи физических величин. Характеристики сигнализационных преобразователей: входные и выходные величины, функция преобразования, чувствительность. Классификация средств обнаружения по типу преобразования физических величин.
19. Структура и принципы построения сигнализационных датчиков, приборов, систем и комплексов. Принципы построения централизованных и автономных сигнализационных систем. Влияние дестабилизирующих факторов на работоспособность сигнализационных датчиков.
20. Сигнализационные датчики охраны режимных помещений и протяженных участков. Классификация, основные характеристики и конфигурация контролируемых зон сигнализационных датчиков.
21. Сигнализационные датчики первого рубежа охраны: электроконтактные, магнитоконтактные, удароконтактные. Основные характеристики и особенности применения активных и пассивных инфракрасных сигнализационных датчиков.
22. Классификация радиотехнических средств обнаружения. Однопозиционные СВЧ-датчики для охраны помещений. Радиотехнические датчики охраны периметра объекта. Блокировка помещений и участков периметров сигнализационными датчиками емкостного типа.
23. Ультразвуковые объемные датчики охраны помещений. Акустические датчики охраны остекленных поверхностей. Контроль поверхностей стен, перекрытий и отдельных предметов с помощью вибрационных сигнализационных датчиков. Периметровые вибрационные и сейсмические датчики.
24. Быстроразвертываемые сигнализационные системы. Датчики охраны периметров с малозаметной линейной частью.
25. Правила размещения на контролируемом объекте сигнализационных датчиков охраны периметров и помещений. Типовые схемы размещения чувствительных элементов сигнализационных датчиков в охраняемых помещениях.
26. Устройства и системы пожарной сигнализации. Классификация и принципы построения пожарных датчиков. Пожарные приемно-контрольные приборы и

сигнально-пусковые устройства. Порядок выбора и установки пожарных датчиков и приемно-контрольных приборов на объектах, требования нормативных документов.

27. Классификация и обобщенная структура телевизионных средств наблюдения. Тактические требования, предъявляемые к системам охранного телевидения.
28. Телевизионная аппаратура передачи и приема, устройства обработки видеоизображения. Анализаторы видеоизображения, видеодетекторы движения.
29. Устройства дистанционного управления видеосистемами. Аппаратура отображения, документирования и архивирования видеоинформации. Вспомогательное оборудование видеосистем.
30. Основные понятия и определения, классификация систем управления доступом. Специальные режимы пропуска.
31. Биометрические системы аутентификации. Биометрическая аутентификация по статическим признакам.
32. Биометрические системы аутентификации. Биометрическая аутентификация по динамическим признакам.
33. Сведения о распознающих приборах, их характеристика. Ошибки первого и второго рода. Хранение аутентифицирующей биометрической информации в базах данных системы управления доступом.
34. Достоинства и недостатки биометрических систем. Перспективные способы аутентификации
35. Физические носители ключевой информации. Устройства хранения и обработки идентифицирующей информации на основе смарт-карт.
36. Исполнительные устройства управления доступом. Механические, электромеханические замки, автоматические шлагбаумы, турникеты, шлюзы.
37. Классификация и основные характеристики приемно-контрольных приборов охранно-пожарной сигнализации. Обобщенная структурная схема приемно-контрольных приборов. Приемно-контрольные приборы многопроводной (лучевой) структуры, принципы контроля состояния двухпроводных шлейфов охранной и пожарной сигнализации, основные типы регистрирующих ячеек.
38. Адресные проводные и радиоканальные приемно-контрольные приборы: протокол обмена данными между приемно-контрольными приборами и периферийными устройствами, способы разделения каналов системы синхронизации. Использование радио- и электросети в качестве адресной линии связи.
39. Системы передачи информации охранно-пожарной сигнализации. Построение систем передачи тревожной информации от периферийных устройств объектовой сигнализации. Принципы построения систем передачи информации, использующих специально выделенные и занятые линии телефонной сети общего пользования.
40. Радиоканальные системы передачи информации: приемо-передающая аппаратура, антенны, выбор частотного диапазона, особенности распространения радиоволн в городских условиях, радиопомехи. Использование радиолиний сотовых сетей связи общего пользования, специальных радиосетей передачи данных.
41. Тактика действия преступников при ограблении инкассаторов и транспортных средств. Полномочия инкассаторов и работников охраны на маршрутах инкассации.
42. ГОСТ Р 50963-96 «Защита броневая специальных автомобилей». Сравнительные характеристики отечественных и зарубежных транспортных средств инкассации.
43. Методы получения информации о возможных нападениях на транспортные средства инкассации.
44. Основные виды угроз безопасности должностных лиц и сотрудников объектов финансовой сферы. Способы осуществления угроз преступниками.
45. Самоохрана должностных лиц и сотрудников объектов финансовой сферы.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России
Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Информационная безопасность финансовой деятельности банков	**Код модуля1140584** **Учебный план №** 6938
Образовательная программа Информационно аналитические системы безопасности	**Код ОП** 10.05.04/01.01
Направление подготовки Информационная безопасность финансовых и экономических структур	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки Высшее образование – специалитет	
ФГОС ВО 10.05.04 Информационно аналитические системы безопасности	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 01.12.2016 №1514

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	К.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам. председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению обеспечения безопасности банковских устройств самообслуживания, в частности банкоматов и платежных терминалов. В дисциплине рассматриваются строение и функционирование платежных терминалов и банкоматов, их классификация и свойства, характеристика составных модулей. Изучаются основные виды угроз, связанных с устройствами самообслуживания банков, возможные категории нарушителей, а также излагаются организационные и технические меры по защите банкоматов и платежных терминалов.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-3);
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);

- способность разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности (ПК-16);

- способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные (ПК-18);
- способность обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей (ПК-19);
- способность анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства (ПК-20).
- способность выполнять анализ корректности и устойчивости функционирования отдельных компонентов, подсистем и в целом всей национальной системы по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма (ПСК-2.2);
-

В результате освоения дисциплины студент должен:

Знать:

- тактико-технические характеристики и принципы работы банкоматов и платежных терминалов;
- категории мест размещения и классификацию банковских устройств самообслуживания;
- угрозы в отношении банкоматов и платежных терминалов, уязвимости программного обеспечения;

- принципы и методы защиты банкоматов и платежных терминалов.
- требования ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов;
- способы противодействия основным видам криминалистических угроз в отношении банковских устройств самообслуживания.

Уметь:

- оценивать полноту обеспечения безопасности платежных терминалов и банкоматов;
- формировать модели нарушителей;
- разрабатывать организационные и технические мероприятия по обеспечению защиты банковских систем самообслуживания;
- фиксировать факты атак и попыток их совершения, осуществлять информирование Банка России;
- осуществлять классификацию преступлений, связанных с незаконным проникновением в зону размещения банковских устройств самообслуживания, криминальными посягательствами на них и конфиденциальную информацию идентификационных электронных карт, а также на пользователей банкоматов и платежных терминалов, инкассаторов и обслуживающий персонал.

Владеть (демонстрировать навыки и опыт деятельности):

- профессиональной терминологией в области обеспечения безопасности платежных терминалов и банкоматов;
- методами категорирования банкоматов и платежных терминалов;
- навыками информирования Банка России об атаках или попыток атак;
- методами обеспечения безопасности банкоматов и платежных терминалов;
- методами расчета оценочных значений времени взлома сейфа.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего Часов	В т.ч. контактная работа (час.)*	*9*
1.	**Аудиторные занятия**	85	85	85
2.	Лекции	51	51	51
3.	Практические занятия	34	34	34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	59	12,75	59
6.	**Промежуточная аттестация**	Э	2,33	Э
7.	**Общий объем по учебному плану, час.**	144		144
8.	**Общий объем по учебному плану, з.е.**	4		4

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в

группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Банковское устройство самообслуживания**	Основная терминология ГОСТ Р 51221-98 Средства защитные банковские. Классификация банковских устройств самообслуживания (БУС) по конструкции, области применения и способу установки. Классификация БУС по материальной ценности, функциональным возможностям. Категорирование мест размещения БУС, категории Р1-Р4.
2	**Банкоматы**	Классификация банкоматов. Структура устройства банкоматов, характеристика основных модулей. Системный блок. Устройства ввода информации, описание сигнального интерфейса, коды команд, алгоритмы работы. Устройства вывода информации. Средства управления. Устройство выдачи банкнот, основные технические характеристики, конструкция, принципы функционирования. Кассеты для хранения банкнот и отказная кассета. Режим работы банкомата. Автономный режим и режим реального времени. Основные технологические этапы работы банкомата. Основные модели и функциональные возможности банкоматов. Мировые производители.
3	**Платежные терминалы**	Классификация платежных терминалов по функциональным возможностям. Агентская и банковская схемы функционирования. Функциональные части и их назначение. Корпус платежного терминала, модем для организации обмена информацией между платежным терминалом и сервером электронной платежной системы. Конструктивные особенности Безопасность платежных терминалов. Этапы работы платежных терминалов.
4	**Основные виды угроз в отношении Банкоматов и платежных терминалов.**	Общие критерии формирования модели нарушителя. Типология нарушителей. Категории нарушителей и виды совершаемых преступлений. Цели нарушителей. Оценка опасности нарушителя исходя из степени его осведомленности, оснащенности и подготовленности, типология нарушителей по подготовленности к преодолению системы охраны. Категории нарушителей и виды совершаемых ими преступлений, связанных с незаконным проникновением в зону размещения банкоматов и платежных терминалов, криминальными посягательствами и конфиденциальную информацию банкоматов, а также на пользователей платежных терминалов и банкоматов, инкассаторов и обслуживающий персонал. Квалификация

		преступления. Угрозы держателю карты, обслуживающему персоналу. Нападение. Неправомерный доступ к Персональным данным. Угрозы банковской карте, ее реквизитам. Скимминг. Шимминг. Траппинг. Угрозы банкоматам и платежным терминалам. Несанкционированное проникновение на территорию, в здание, где установлены платежные терминалы и банкоматы. Вскрытие банкоматов. Хищение, срыв с места установки.
5	**Обеспечение безопасности платежных терминалов и банкоматов**	Требования Положения ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов. Основные организационные и технические меры по защите информации банкоматов и платежных терминалов. Выбор мест размещения банковских устройств самообслуживания. Влияние категории на место размещения. Анализ уязвимостей программного обеспечения банкоматов и терминалов. Обеспечение фиксации. Инженерно-техническая укрепленность и оборудование техническими средствами охраны банковских устройств самообслуживания и мест их размещения. Регулирование и установка порядков срока хранения информации, обновления версий, работы с клиентами. Оценка времени взлома. Минимальные требования по устойчивости к взлому сейфов. Регистрация доступа к банкоматам и платежным терминалам. Использование видеонаблюдения для регистрации доступа (Возможные схемы использования). Контроль положения, линий связи. Системы удаленного мониторинга состояния устройства, обеспечивающие контроль надлежащего функционирования защитного оборудования и специального программного обеспечения. Требования к системе передачи тревожных сообщений для защиты банкоматов и платежных терминалов. Фиксация фактов атак и попыток их совершения. Информирование Банка России. Информирование населения.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 12
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноя. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Банковское устройство самообслуживания	7	5	5			2	2	2																					
2	Банкоматы	20	12	8	4		8	5	3		2														3	1					
3	Платежные терминалы	22	13	8	5		9	6	4		2														3	1					
4	Основные виды угроз в отношении банкоматов и платежных терминалов	28	20	9	11		8	8	3		5																				
5	Обеспечение безопасности платежных терминалов и банкоматов	32	18	4	14		14	8	4		4		6	1																	
	Всего (час), без учета промежуточной аттестации:	109	68	34	34		41	29	16		13		6	6											6	6					
	Всего по дисциплине (час.):	**144**	**68**				**58**	В т.ч. промежуточная аттестация																				**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Этапы взаимодействия с банкоматами.	4
3	2	Этапы взаимодействия с платежными терминалами.	5
4	3	Разработка модели нарушителя.	5
4	4	Сопоставление вида совершаемых преступлений и статей уголовного кодекса Российской Федерации.	6
5	5	Составление рекомендаций по обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов.	7
5	6	Разработка методики и протокола информирования центрального аппарата при возникновении попыток атак.	7
		Всего:	**34**

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

– *Разработка основных организационных и технических мер по физической защите банкоматов и платежных терминалов.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

– *Основные элементы банкоматов и их функции.*

– *Основные элементы платежных терминалов и их функции*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Банковское устройство самообслуживания			*	*	*							
2.Банкоматы				*				*				
3.Платежные терминалы					*			*				
4.Основные виды угроз в отношении Банкоматов и платежных терминалов				*	*						*	
5.Обеспечение безопасности платежных терминалов и банкоматов					*						*	

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Артемов, А.В. Информационная **безопасность** : курс лекций / А.В. Артемов ; Межрегиональная Академия **безопасност**и и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605

2. Мошенничество в платежной сфере: бизнес-энциклопедия / Центр исследований платежных систем и расчетов ; ред.-сост. А. Воронин. - Москва : Интеллектуальная Литература, 2016. - 345 с. : табл., схем. - ISBN 978-5-99072-232-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=430951
3. Криворучко, С.В. Национальная платежная система: структура, технологии, регулирование. Международный опыт, российская практика : монография / С.В. Криворучко, В.А. Лопатин. - Москва : ЦИПСиР, 2013. - 456 с. - ISBN 978-5-406-02867-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=235078
4. Гаврилов, Л.П. Основы электронной коммерции и бизнеса : учебное пособие / Л.П. Гаврилов. - Москва : СОЛОН-ПРЕСС, 2009. - 592 с. : ил. - (Библиотека студента). - ISBN 978-5-91359-065-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=118188

9.1.2.Дополнительная литература

1. Лямин, Л.В. Применение технологий электронного банкинга: риск-ориентированный подход / Л.В. Лямин. - Москва : КНОРУС : ЦИПСиР, 2011. - 333 с. - ISBN 978-5-406-00978-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=209473
2. Национальный Банковский Журнал / гл. ред. А. Скогорева - Москва : ООО УК «Национальный Банковский Журнал», 2015. - № 2(130). - 114 с.: ил. - ISSN 1810-2913 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428568

9.2.Методические разработки

Не предусмотрено

9.3.Программное обеспечение

MS Office

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа №1	*10,1-7*	*25*
Контрольная работа №2	*10,1-7*	*25*
Домашняя работа	*10,8-15*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическая работа №1	*10,1-7*	*15*
Практическая работа №2	*10,1-7*	*15*
Практическая работа №3	*10,1-7*	*15*
Практическая работа №4	*10,8-15*	*15*
Практическая работа №5	*10,8-15*	*20*
Практическая работа №6	*10,8-15*	*20*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 10	**1**

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с наличием Дисциплины и ее аналогов, по которым возможно тестирование, на портале СМУДС УрФУ, возможно тестирование в рамках НТК.

ПРИЛОЖЕНИЕ 3

к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	Пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Классификация банковских устройств самообслуживания.
2. Категорирование мест размещения банковских устройств самообслуживания.
3. Банкоматы. Классификация по функциональным возможностям.
4. Структура и характеристик основных модулей банкоматов.
5. Режимы работы банкоматов.
6. Банкоматы. Устройство выдачи банкнот, основные характеристики, конструкция.
7. Основные технологические этапы работы банкомата.
8. Основные модели и производители банкоматов.
9. Классификация платежных терминалов по функциональным возможностям.
10. Основные технологические этапы работы платежных терминалов.
11. Категории нарушителей и цели нарушителей при моделировании угроз банкоматов и платежных терминалов.
12. Категории нарушителей и виды совершаемых ими преступлений.
13. Анализ уязвимостей программного обеспечения и порядок их устранения.
14. Криминалистический характер нарушений в отношении банкоматов и платежных терминалов.
15. Угрозы банковской карте, ее реквизитам. Скимминг. Шимминг. Траппинг.
16. Несанкционированное проникновение на территорию, где установлены платежные терминалы и банкоматы.
17. Требования Положения ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов.
18. Регистрация доступа к банкоматам и платежным терминалам. Использование видеонаблюдения.
19. Порядок ремонта терминалов, обеспечение безопасности банкоматов. Порядок снятия с эксплуатации.
20. Регулирование порядка работы платежных терминалов и банкоматов.

21. Требования к системе передачи тревожных сообщений для защиты банкоматов и платежных терминалов.
22. Информирование населения об угрозах.
23. Порядок доступа к банкоматам и платежным терминалам.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено